



UNITED STATES MARINE CORPS
MARINE CORPS RECRUITING COMMAND
3280 RUSSELL ROAD
QUANTICO, VA 22134-5103

IN REPLY REFER TO:
2000
MCRC
FEB 3 2004

COMMANDING GENERAL'S POLICY LETTER 2-04

From: Commanding General

Subj: MARINE CORPS PERSONNEL APPROPRIATE USE OF GOVERNMENT
INFORMATION TECHNOLOGY (IT) RESOURCES

Ref: (a) ALMAR 388/97
(b) MARADMIN 541/99
(c) MARADMIN 162/00
(d) COMMARFOR CND message 041600Z Aug 00
(e) DOD GENERAL COUNSEL MEMO of 27 Mar 1997

Encl: (1) Statement of Understanding for Computer Use

1. The references are used as general guidance to provide a framework for Marine Corps Recruiting Command (MCRC) personnel use of the Internet and email services. The references provide sound direction regarding permissible and prohibited use of the Internet and email services by everyone assigned to Marine Corps commands who use government equipment and/or connect to government networks.

2. The Internet, specifically the World Wide Web (WWW), is a valuable tool for obtaining and disseminating information. When used effectively, it can facilitate Marine Corps information management needs and enhance our productivity.

3. MCRC is connected to the Recruiting Services Network (RSN). The configuration of the RSN network dictates that all MCRC Internet traffic is routed from Recruiting Stations (RS) and Marine Corps Districts (MCD) through the MCRC Headquarters and out to the Internet. This structure is in place for both financial and security reasons. MCRC uses the RSN to speed mission critical information to decision makers throughout the command. The resources of the network through which we share access to the Internet are both limited and expensive. Therefore, users should ensure use is aligned to unit missions and goals.

Subj: MARINE CORPS PERSONNEL APPROPRIATE USE OF GOVERNMENT
INFORMATION TECHNOLOGY (IT) RESOURCES

4. **Government Information Technology resources are for official use and authorized purposes only.** Marine Corps resources in the form of computer hardware, software, and telecommunication infrastructure that facilitate use of Internet and email services can be used when work-related and determined to be in the best interests of the Government and the Marine Corps. Access should be appropriate in the frequency, duration, and related to assigned tasks. MCRC has placed limits to the number and types of information files (text, pictures, etc.) it can transport. Too many users simultaneously sending and/or receiving large files degrades network performance and denies access to other official users. These conditions demand that we discipline our use of the network with regard to the sites we access and the size of the files we transmit and download.

5. Marine Corps assets may be used to access the Internet for incidental personal purposes. Users are reminded that on a Government owned network, no expectation of privacy exists. Users browsing habits and email content may be subject to logging and screening. Personal use such as Internet searches and brief communications are permitted as long as such use:

a. Does not adversely affect the performance of official duties by the Marine/employee.

b. Serves a legitimate Marine Corps interest such as enhancing professional skills.

c. Is of minimal frequency and duration and occurs during an individual's personal time.

d. Does not overburden Government computing resources or communication systems.

e. Does not result in added costs to the Government.

f. Is not used for purposes that adversely reflect upon the Marine Corps.

6. The references delineate examples of Internet use and email service that are prohibited. In addition to those examples, any Internet activity that places uninterrupted demand on the network infrastructure is likewise prohibited. Examples include, "tickertape" ball scores, "real audio" radio broadcasts and stock market quotes that provide a continuous stream of updated information to the subscriber.

Subj: MARINE CORPS PERSONNEL APPROPRIATE USE OF GOVERNMENT
INFORMATION TECHNOLOGY (IT) RESOURCES

7. All MCRC users will be educated on the use of the Internet and email services by attending annual Information Assurance training. Prior to being issued an account and password and before utilizing a DoD computer system, all users will sign and date the most recent version of the Statement of Understanding for Computer Use [enclosure (1)].

8. Violation of this policy may result in administrative or disciplinary action, to include nonjudicial punishment or courts-martial. The MCRC G-6 monitors network usage and takes appropriate action when unauthorized use is suspected. Unauthorized use will be investigated and individuals in violation of this policy will be held accountable.

9. The appropriate use of government information technology resources is a leadership issue that requires both education and vigilance. When in doubt, remember that all Internet and email traffic, both authorized and unauthorized, competes with all MCRC users throughout the country for precious network bandwidth. Be prudent, be smart, be conscientious.


C. CORTEZ

DISTRIBUTION: A, D

STATEMENT OF UNDERSTANDING FOR COMPUTER USE

NOTICE AND CONSENT LOG-ON BANNER

"THIS IS A DEPARTMENT OF DEFENSE (DOD) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, TO INCLUDE ENSURING THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES." (REFERENCE: DOD GENERAL COUNSEL MEMO, DATED 27 MAR 1997 APPLIES)

USER RESPONSIBILITY AGREEMENT

As a NIPRNET user, I understand that I am responsible and accountable for following all requirements of this agreement. I am solely responsible for all access and actions carried out under my user identification and password. As part of my responsibilities: (Read and initial the following)

1. I have read and understand the notice and consent "log-on banner" that appears on the front of this document and is displayed on USMC computers. I understand that logging into the RSN constitutes consent to auditing and monitoring at all times. _____(Initials)
2. I have received training on the USMC's acceptable use policy. I will adhere to all security policies concerning external connectivity. _____(Initials)
3. I understand that I am solely responsible for all access and actions carried out under my user identification (User ID) and password. _____(Initials)
4. The RSN is an unclassified network. I will not enter or process any classified information on the RSN or any other unclassified system or network. _____(Initials)
5. I will not disclose my password to anyone due to reassignment, transfer or termination. I will not write my password down or transmit it electronically. _____(Initials)
6. I will limit the use of the RSN to official and authorized use and not utilize the RSN for unauthorized or prohibited use. _____(Initials)
7. I will notify my ISC or the MCRC G-6 immediately of any computer security incidents such as viruses, loss or compromise of my password, suspected system tampering or computer hacking, etc. _____(Initials)
8. I will not circumvent security requirements to obtain unauthorized access (such as change system configuration files, disable anti-virus software). _____(Initials)
9. I will not connect to commercial Internet Service Providers (ISPs) mail systems nor will I send government data via a commercial ISP (AOL, HOTMAIL, etc.). _____(Initials)
10. I understand that games and unauthorized software are not permitted on computers connected to the RSN. _____(Initials)
11. I will adhere to all INFOCON measures as promulgated for the current INFOCON level. _____(Initials)
12. I understand that remote access is authorized only for official government use that is required for my job assignment. I will not use remote access for unofficial web browsing or email. _____(Initials)
13. I understand that I must notify my ISC and MCRC G-6 upon termination or transfer. _____ (Initials)

I UNDERSTAND THAT FAILURE TO ADHERE TO PUBLISHED POLICIES WILL RESULT IN IMMEDIATE SUSPENSION OF MY ACCOUNT AND CAN RESULT IN DISCIPLINARY OR ADMINISTRATIVE ACTION.

USER NAME (PRINT):

DATE:

USER SIGNATURE:

Enclosure (1)